

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA**

Alauntae Butts and Marquese York,
individually and on behalf all others
similarly situated,

Plaintiffs,

v.

Fortra LLC,

Defendant.

CASE NO. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Alauntae Butts and Marquese York (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this action against Defendant Fortra LLC (“Defendant”), a Minnesota-based Limited Liability Company, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the targeted cyberattack and data breach in January 2023 (“Data Breach”) on Defendant’s network that resulted in unauthorized access to its customer and employee data. As a result of the Data Breach, Plaintiffs and approximately 139,493 Class Members¹ suffered ascertainable losses, including the loss of

¹<https://apps.web.main.gov/online/aeviwer/ME/40/4cfbf86f-8d04-4296-9195-81b874ba939a.shtml> (last visited: March 14, 2023).

the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. In addition, the sensitive personal information Plaintiff and Class Members entrusted to Defendant was compromised and unlawfully accessed through the Data Breach.

3. Information compromised in the Data Breach includes Defendant's customers' and employees' names and Social Security number (collectively, "Private Information").

4. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of the Private Information that Defendant collected and stored.

5. Plaintiffs and Class Members provided their Private Information to Hatch Bank who, upon information and belief, contracted with Defendant to store and protect Plaintiffs and Class Members' Private Information.

6. As explained below, Defendant's inadequate cybersecurity measures enabled an unauthorized third party to gain access to Defendant's network and obtain Plaintiffs and Class Members' Private Information.

7. On or around February 28, 2023, Plaintiffs received a Notice of Security Incident ("Notice of Data Breach"), which informed them of the following:

What Happened? On January 29, 2023, [Defendant] experienced a cyber incident when they learned of a vulnerability located in their software. On February 3, 2023, Hatch Bank was notified by [Defendant] of the incident and learned its files contained on [Defendant's] GoAnywhere site were subject to unauthorized access. [Defendant's] investigation determined that,

between January 30 and January 31, 2023, someone without authorization had access to certain files stored within [Defendant'] GoAnywhere site. [Defendant] launched a diligent and comprehensive review of relevant files to determine the information that may have been impacted.

What Information was Involved? On February 7, 2023, [Defendant] determined the information may have been impacted by this incident includes [Plaintiffs'] name and Social Security number. Again, at this time [Defendant] has no indication that your information was subject to an actual or attempted misuse as a result of this incident.

8. Through its Notice of Data Breach, Defendant admits that the Data Breach was caused, at least in part, due to “vulnerability[ies] located in [its] software.”

9. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

10. Because of Defendant's negligent conduct, Plaintiffs and Class Members' identities are now at risk because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes victimizing Plaintiffs and Class Members, including, opening new financial accounts in their names, taking out loans in their names, using their

names to obtain medical services, obtaining driver's licenses in their names with a different photograph, and giving false information to police during an arrest.

12. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members now must, at a minimum, closely monitor their financial accounts to guard against identity theft, from now until an unforeseeable point in the future.

13. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. In bringing this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was unlawfully accessed during the Data Breach.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

16. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims on behalf of the Class (defined *infra*) for negligence and negligence *per se*.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum

or value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

18. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the many of the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

19. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District

PARTIES

20. Plaintiff Alauntae Butts is, and at all times mentioned herein was, an individual citizen of the State of Iowa. Plaintiff received a data breach notice letter dated February 28, 2023 informing her that her Private Information, such as her name and Social Security Number, had been compromised.

21. Plaintiff Marquese York is, and at all times mentioned herein was, an individual citizen of the State of California. Plaintiff York also received an email with a data breach notice in or around February 2023 informing him that his Private Information, such as his name and Social Security Number, had been compromised.

22. Defendant Fortra LLC is a limited liability company organized and registered according to the laws of the State of Delaware. Defendant maintains its primary headquarters in Eden Prairie, Minnesota. Defendant's principal place of business is located at 11095 Viking Drive, Suite 100, Eden Prairie, Minnesota, 55344.

DEFENDANT'S BUSINESS

23. Defendant provides information technology management software and services. The Company offers automation, cybersecurity, monitoring solutions, product training, implementation, configuration, upgrades, conversion services. Help/Systems serves customers worldwide.²

24. On its website, Defendant refers to itself as “Your Cybersecurity Ally” and offers services such as vulnerability management, offensive security, email security & anti-phishing, data protection, digital risk protection, and secure file transfer.³

25. On information and belief, in the ordinary course of business, Defendant contracts with companies to store and protect client information, such as names and Social Security numbers.

26. On information and belief, Plaintiffs and Class Members provided their Private Information to Hatch Bank who, in turn, hired Defendant to store and protect Plaintiffs and Class Members’ Private Information.

27. By accepting Plaintiffs and Class Members’ Private Information, Defendant promised to provide confidentiality and adequate security for this Private Information.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class Members’ Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs and Class Members’ Private Information from unauthorized disclosure.

² <https://www.bloomberg.com/profile/company/6721124Z:US?leadSource=uverify%20wall> (last visited: March 14, 2023).

³ <https://www.fortra.com> (last visited: March 14, 2023).

29. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

30. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK AND DATA BREACH

31. Defendant experienced a Data Breach on or around January 29, 2023.

32. On February 3, 2023, Defendant notified Hatch Bank that its systems had been subject to the Data Breach. Specifically, Defendant stated that an actor had gained unauthorized access to Defendant's network.

33. On February 7, 2023, Defendant determined that information on its systems may have included names and Social Security numbers.

34. On information and belief, the investigation revealed that approximately 139,493 individuals had their information accessed as a result of the Data Breach.⁴

35. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

36. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the breach.

⁴ <https://apps.web.maine.gov/online/aewviewer/ME/40/4cfbf86f-8d04-4296-9195-81b874ba939a.shtml> (last visited: March 6, 2023).

37. In light of recent high-profile data breaches at other companies similar to Defendant, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

38. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”⁵

39. In fact, according to the cybersecurity firm PurpleSec, ransomware “has become a popular form of attack in recent years growing 350% in 2018,” and “up 64% year-over-year” in the first half of 2021. a survey of 1,100 IT professionals showed 90% of clients had suffered a ransomware attack in the past year.⁶

40. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

50. The Federal Trade Commission (“FTC”) has promulgated numerous guides

⁵ *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited Mar. 15, 2023).

⁶ *2021 Cyber Security Statistics, The Ultimate List of Stats, Data, & Trends for 2023*, <https://purplesec.us/resources/cyber-security-statistics/#Ransomware> (last visited Mar. 15, 2023).

for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.⁷ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.⁸

52. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

53. The FTC has brought enforcement actions against businesses for failing to

⁷ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting-personal-information.pdf (last visited Aug. 24, 2021).

⁸ *Id.*

adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”). 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

54. Defendant failed to properly implement basic data security practices.

55. Defendant’s failure to employ reasonable and appropriate measures to protect against and detect unauthorized access to customers’ Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

56. Defendant was at all times fully aware of its obligation to protect the Private Information of their customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

57. As shown above, several best practices have been identified that a minimum should be implemented by businesses like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

58. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports;

protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

59. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

60. These foregoing frameworks are existing and applicable industry standards in the any industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

DEFENDANT'S BREACH

61. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;
- b. Failing to adequately protect customers' Private Information;

- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- h. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and
- i. Failing to adhere to industry standards for cybersecurity.

62. Defendant negligently and unlawfully failed to safeguard Plaintiffs and Class Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Private Information.

63. Accordingly, as outlined below, Plaintiffs and Class Members now face a present and substantially increased risk of fraud and identity theft. In addition, Plaintiffs

and the Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at a Present and Substantially Increased Risk of Fraud and Identity Theft

64. Cyberattacks and data breaches at companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

65. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.⁹

66. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.¹⁰

67. The United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”¹¹

⁹ See Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), <https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks> (last visited Aug. 24, 2021).

¹⁰ See Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at <https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203> (last visited Aug. 25, 2021).

¹¹ See U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at <https://www.gao.gov/new.items/d07737.pdf> (last visited Aug. 25, 2021).

68. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal Private Information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

69. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.¹²

¹² See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/#/Steps> (last visited Aug. 25, 2021).

70. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

71. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

72. Moreover, theft of Private Information is also gravely serious. Private Information is an extremely valuable property right.¹³

73. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

74. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

¹³ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

75. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

76. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

77. There is a strong probability that entire batches of information stolen from Defendant have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at a present and substantially increased risk of fraud and identity theft for many years into the future.

78. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

79. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.¹⁴ Private Information particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

¹⁴ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Aug. 25, 2021).

80. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.¹⁵ Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.¹⁶ Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

81. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

82. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”¹⁷

83. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained,

¹⁵ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Aug. 25, 2021).

¹⁶ *Id* at 4.

¹⁷ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Aug. 25, 2021).

“[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”¹⁸

84. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

Plaintiffs' Experience

85. Plaintiffs provided their Private Information to Hatch Bank who, on information and belief, contracted with Defendant to store Plaintiffs' and Class Members' private Information.

86. In or around February 2023, Plaintiffs received a Notice of Data Breach from Defendant informing them that their Private Information had been impacted by the Data Breach.

87. As a result of the Data Breach, Defendant directed Plaintiffs to take certain steps to protect their Private Information and otherwise mitigate their damages.

88. As a result of the Data Breach and the information that they received in the Notice Letter, Plaintiffs have spent significant time dealing with the consequences of the Data Breach, such as self-monitoring their bank and credit accounts, spending time verifying the legitimacy of communications with their banks, exploring credit monitoring

¹⁸ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Aug. 25, 2021).

and identity theft insurance options, and signing up for the credit monitoring supplied by Defendant. This time has been lost forever and cannot be recaptured.

89. Plaintiffs are very careful about sharing their own Private Information and have never knowingly transmitted unsecure Private Information over the internet or any other unsecured source.

90. Plaintiffs strive to store any and all documents containing Private Information in a secure location, including destroying or securing any communications or documents that contain Private Information or that may contain any information that could otherwise be used to compromise their identities and privacy. Moreover, they prudently strive to use unique usernames and passwords and other security measures in various online accounts.

91. Plaintiffs suffered actual injury and damages due to Defendant's mismanagement of their Private Information before the Data Breach.

92. Plaintiffs suffered actual injury in the form of damages and diminution in the value of their Private Information—a form of intangible property that they had entrusted to Defendant, which was compromised in and as a result of the Data Breach.

93. Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and they have suffered anxiety surrounding increased concerns over the theft of their identities and invasion of their privacy. The theft of their full names being paired with their social security numbers, and the unknowns surrounding when and how that information will be used, are especially concerning for Plaintiffs.

94. Plaintiffs have suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and other misuse of their sole Private Information—especially their Social Security numbers being placed in the hands of unauthorized third-parties and possibly criminals.

95. Plaintiffs have a continuing interest in ensuring that their Private Information—which, upon information and belief, Defendant continues to hold—is protected and safeguarded from future breaches.

Plaintiffs and Class Members' Damages

97. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

98. Defendant has merely offered Plaintiffs and Class Members complimentary fraud and identity monitoring services for up to twelve months, but this does nothing to compensate them for damages already incurred, those that could potentially arise from future misuse of their leaked Private Information, nor the time they have spent and will continue to spend dealing with the Data Breach.

99. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

100. Plaintiffs' Private Information was compromised in the Data Breach and is now in the hands of, at the very least, the cybercriminals who accessed Defendant's computer system.

101. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach.

102. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft, among others.

103. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to expend time addressing the effects of the Data Breach in attempt to minimize their losses.

104. Plaintiffs and Class Members face the present and substantially increased risk of out-of-pocket fraud losses, such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar forms of identity theft.

105. Plaintiffs and Class Members face the present and substantially increased risk of being targeted for future phishing, data intrusion, and other illegal schemes based on the release of their Private Information, as fraudsters could use that information to more effectively target Plaintiffs and Class Members in future schemes.

106. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

107. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cybercriminals in the Data Breach. Numerous courts have recognized damages for such propriety of loss of value in similar cases.

108. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiffs and Class Members overpaid for a service or product that was intended

and represented to be accompanied by adequate data security measures, but evidently was not. Part of the price Plaintiffs and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of the Private Information Defendant stored on its networks. Thus, Plaintiffs and the Class Members did not get what they paid for and agreed to.

109. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their various medical accounts and records for misuse of their sensitive information.

110. Plaintiffs and Class Members have suffered and/or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

111. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

112. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to anyone or everyone, thereby subjecting them to embarrassment and depriving them of any right to any privacy whatsoever.

CLASS ACTION ALLEGATIONS

113. Plaintiffs brings this action on behalf of themselves and on behalf of all other persons similarly situated (“the Class”).

114. Plaintiffs proposes the following Class definition, subject to amendment as appropriate:

All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a Notice of Data Breach (the “Class”).

115. The proposed Class is referred to collectively as the “Class.” Members of the Class are referred to collectively as “Class Members.”

116. Excluded from the Class are Defendant’s officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

117. Plaintiffs reserve the right to amend or modify the Class definition as this case progresses.

118. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 7,500 individuals whose Private Information was compromised in the Data Breach.

119. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs and Class Members’ Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- h. Whether Defendant should have discovered the Data Breach sooner;
- i. Whether Defendant's conduct was negligent;
- j. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's negligence;
- k. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;
- l. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- m. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, treble damages, and/or injunctive relief.

120. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

121. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions.

122. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action carries advances the interests of judicial economy, among others.

123. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would also create a risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. In contrast, litigating this matter as a class action presents far fewer management difficulties, conserves judicial and party resources, and protects the rights of each Class Member.

124. Defendant has acted on grounds that apply generally to the Class as a whole, such that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

COUNT I NEGLIGENCE (On Behalf of Plaintiffs and All Class Members)

124. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

125. Defendant required Plaintiffs and Class Members to submit non-public personal information as a condition of employment (or prospective employment) and/or as a condition of purchasing goods and services from Defendant.

126. Defendant had a duty to exercise reasonable care in collecting and storing this data, including using reasonable means to secure and safeguard its computer property—and the Class Members' Private Information held within it—from unauthorized disclosure, as well as to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

127. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

128. Defendant's duty of care to use reasonable security measures arose because Defendant was able to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from the Data Breach.

129. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. 15 U.S.C. § 45.

130. Defendant breached its duties, and therefore was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to timely notify Class Members about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- g. Failing to have mitigation and back-up plans in place in the event of a

cyber-attack and data breach.

131. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the well-known high frequency of cyberattacks and data breaches in the past few years.

132. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in numerous injuries to Class Members.

133. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

134. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and All Class Members)

135. Plaintiffs re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

136. Pursuant to Section 5 of the Federal Trade Commission Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information. 15 U.S.C. § 45.

137. Plaintiffs and Class Members are within the class of persons that the FTCA was intended to protect.

138. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses that, due to their failure to employ reasonable data security measures and abstain from unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class here.

139. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

140. Defendant's violations of the FTCA constitutes negligence *per se*.

141. But for Defendant's negligent breach of the duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

142. The injury and harm suffered by Plaintiffs and Class Members was a reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was acting in violation of the law and in breach of its duties, and that such breaches would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

143. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for judgment as follows:

- a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class counsel;
- b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and Class Members' Private Information;
- c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;
- f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties as allowable by law in an amount to be determined;
- g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- h) Pre- and post-judgment interest on any amounts awarded; and
- i) Such other relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demands a trial by jury on all claims so triable.

Dated: March 15, 2023

Respectfully Submitted,

/s/ David A. Goodwin

Daniel E. Gustafson (MN Lic. #202241)

David A. Goodwin (MN Lic. #0386715)

Joe E. Nelson (MN Lic. #0402378)

GUSTAFSON GLUEK PLLC

120 South Sixth Street, Suite 2600

Minneapolis, MN 55402

Tel: (612) 333-8844

dgustafson@gustafsongluek.com

dgoodwin@gustafsongluek.com

jnelson@gustafsongluek.com

John G. Emerson
Emerson Firm, PLLC
2500 Wilcrest Drive, Suite 300
Houston, TX 77042-2754
Tel: (800) 51-8649
Fax: (501) 286-4659
jemerson@emersonfirm.com

Pro hac vice forthcoming

Attorneys for Plaintiffs and the Proposed Class